English Abstract

23oct07 13:16:00 User266881 Session D3185.2
Sub account: 42933/306360

SYSTEM:OS - DIALOG OneSearch
File 345:Inpadoc/Fam.& Legal Stat 1968-2007/UD=200741
(c) 2007 EPO
***File 345: August 27, 2007 - reloaded with new and enhanced content.**
See HELP NEWS 345 for details.
File 351:Derwent WPI 1963-2007/UD=200767
(c) 2007 The Thomson Corporation

Set	Items	Description
S1	2	PN=JP 11282804

1/5/2 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

0009719520 - Drawing available
WPI ACC NO: 2000-004219/ **20 00** 01
XRPX Acc No: N2000-003665
User authentication system for client-server system connected to internet - transmits completed authentication information to client when user authentication is successful
Patent Assignee: SECOM JOHO SYSTEM KK (SECO-N)
Inventor: HIRAI S
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update
JP 11282804	A	19991015	JP 199885319	A	19980331	200001 B

Priority Applications (no., kind, date): JP 199885319 A 19980331

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
JP 11282804	A	JA	11	6	

Alerting Abstract JP A
NOVELTY - When receiving access from a client (12) which is not finished the user authentication, a redirect demand information is transmitted for accessing web authentication server (16) to perform user authentication of client. When the user authentication is successful, a completed authentication information indicating that user authentication of client is successful, is transmitted. DETAILED DESCRIPTION - When completed authentication information is transmitted to client, a redirect demand information for accessing web service server (10) collectively is transmitted. An INDEPENDENT CLAIM is also included for the user authentication procedure.
USE - For client-server system connected to internet.
ADVANTAGE - As user authentication is performed directly between client and authentication server, interdependence relationship of web service server and authentication server is reduced, hence versatility of authentication server is enhanced with simple authentication system.
DESCRIPTION OF DRAWING(S) - The figure shows schematic component of

communication system. (10) Web service server; (12) Client; (16) Authentication server.

Title Terms/Index Terms/Additional Words: USER; AUTHENTICITY; SYSTEM; CLIENT; SERVE; CONNECT; TRANSMIT; COMPLETE; INFORMATION; SUCCESS

Class Codes
International Classification (Main): G06F-015/00
(Additional/Secondary): H04L-012/54, H04L-012/58, H04L-009/32

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-J; W01-A03B; W01-A05B; W01-A06G2

1/39/1 (Item 1 from file: 345)
DIALOG(R)File 345:Inpadoc/Fam.& Legal Stat
(c) 2007 EPO. All rts. reserv.

53976375 Family ID: 23976376
<No. of Patents: 1> <No. of Countries: 1>
Patent Basic (No,Kind,Date): JP 11282804 A 19991015
COMMUNICATION SYSTEM HAVING USER AUTHENTICATION FUNCTION AND USER AUTHENTICATION METHOD (English)
Patent Assignee: SECOM JOHO SYSTEM KK
Author (Inventor): HIRAI SHIGERU
***

Patent Family:

Patent No	Kd	Date	Applic No	Kd	Date	Wk	Added
JP 11282804	A	19991015	JP 199885319	A	19980331	199948	(B)

Priority Data (No,Kind,Date):
JP 199885319 A 19980331

******* JAPAN (JP) *******
JAPAN (JP) PATENT(S):
Patent (No,Kind,Date): JP 11282804 A 19991015
COMMUNICATION SYSTEM HAVING USER AUTHENTICATION FUNCTION AND USER AUTHENTICATION METHOD (English)
Patent Assignee: SECOM JOHO SYSTEM KK
Author (Inventor): HIRAI SHIGERU
Priority (No,Kind,Date): JP 199885319 A 19980331
Applic (No,Kind,Date): JP 199885319 A 19980331
IPC + Level Value Position Status Version Action Source Office

v. 6 main:	G06F-015/00						
v. 6 :	H04L-009/32						
v. 6 :	H04L-012/54						
v. 6 :	H04L-012/58						
v. 8 adv :	G06F-0015/00	A I	R	20060101	20051110	M	EP
v. 8 adv :	G06F-0021/20	A I F	R	20060101	20051220	M	JP
v. 8 adv :	H04L-0009/32	A I L	R	20060101	20051220	M	JP
v. 8 adv :	H04L-0012/54	A I	R	20060101	20051110	M	EP
v. 8 adv :	H04L-0012/58	A I	R	20060101	20051110	M	EP
v. 8 core:	G06F-0015/00	C I	R	20060101	20051110	M	EP
v. 8 core:	G06F-0021/20	C I F	R	20060101	20051220	M	JP
v. 8 core:	H04L-0009/32	C I L	R	20060101	20051220	M	JP
v. 8 core:	H04L-0012/54	C I	R	20060101	20051110	M	EP
v. 8 core:	H04L-0012/58	C I	R	20060101	20051110	M	EP

Date of Availability: 19991015 Unexamined printed without grant
Language of Document: Japanese
Update Week: Backfile (First Week Added: 199948)

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－282804

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ａ
	12/54				６７５Ｄ
	12/58			11/20	１０１Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－85319

(22)出願日　平成10年(1998)３月31日

(71)出願人　596143657
セコム情報システム株式会社
東京都三鷹市下連雀８丁目10番16号　セコム情報システム株式会社内

(72)発明者　平井　滋
東京都三鷹市下連雀８－10－16　セコム情報システム株式会社内

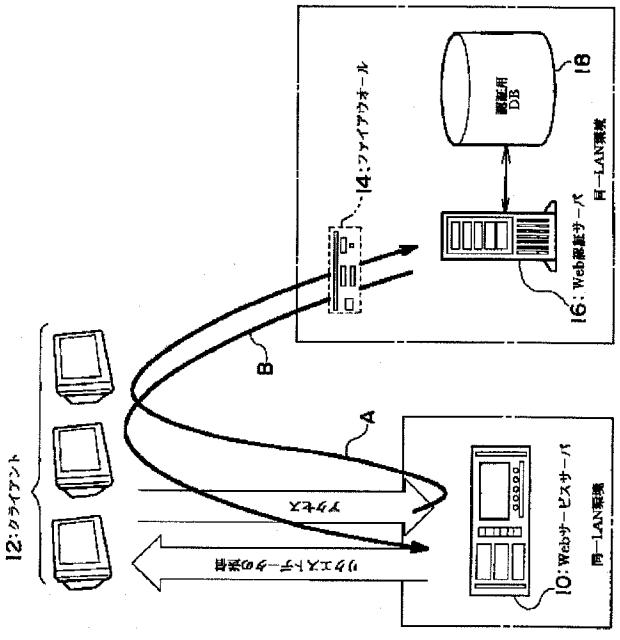
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　ユーザ認証機能付き通信システム及びユーザ認証方法

(57)【要約】

【課題】　サービスサーバと認証サーバとの独立性及び汎用性を高め、認証サーバを複数のサービスで共通利用することが容易な認証システムを提供する。

【解決手段】　ユーザ認証を終えていないクライアント１２からアクセスを受けた場合、Ｗｅｂ認証サーバ１６にアクセスしてユーザ認証を済ませるよう、リダイレクト要求を含むＷｅｂページをクライアント１２に返信する。クライアント１２がこれを受けてＷｅｂ認証サーバ１６にアクセスすれば、該Ｗｅｂ認証サーバ１６では必要な認証処理を行い、認証に成功すればその旨をクッキーに設定してクライアント１２に所定Ｗｅｂページを返信する。この際、このＷｅｂページに再度Ｗｅｂサービスサーバ１０にアクセスさせるためのリダイレクト要求を含めてもよい。こうすれば、Ｗｅｂサービスサーバ１０とＷｅｂ認証サーバ１６との直接のアクセスを無くして、Ｗｅｂ認証サーバ１６の独立性、汎用性を高めることができる。



【特許請求の範囲】
【請求項１】　ネットワーク上に相互に通信可能に接続されたサービスサーバ、認証サーバ、及びクライアントを含むシステムにおいて、
前記サービスサーバは、必要なユーザ認証を終えていない前記クライアントからアクセスを受けた場合に、該クライアントに対して前記認証サーバにアクセスするよう要求するリダイレクト要求情報を送信する手段を含み、
前記認証サーバは、前記クライアントからアクセスがあった場合に該クライアントのユーザ認証を行い、前記ユーザ認証が成功した場合にユーザ認証が成功したことを表す認証済み情報を前記クライアントに送信する手段を含む、
ことを特徴とする通信システム。
【請求項２】　請求項１に記載の通信システムにおいて、
前記認証サーバに含まれる前記手段は、前記認証済み情報を前記クライアントに送信する際に、併せて前記サービスサーバにアクセスするよう要求するリダイレクト要求情報を送信する、ことを特徴とする通信システム。
【請求項３】　請求項１又は２に記載の通信システムにおいて、
前記クライアントは、前記サービスサーバ又は前記認証サーバからリダイレクト要求情報を受信した場合に前記サービスサーバ又は前記認証サーバにアクセスする手段を含むことを特徴とする通信システム。
【請求項４】　請求項１乃至３のいずれかに記載の通信システムにおいて、
前記クライアントは、前記認証サーバから既に前記認証済み情報を受信している場合に、前記サービスサーバへのアクセスの際に前記認証済み情報を該サービスサーバに送信する手段をさらに含むことを特徴とする通信システム。
【請求項５】　ネットワーク上に相互に通信可能に接続されたサービスサーバ、認証サーバ、及びクライアントを含むシステムにおいて前記クライアントのユーザ認証を行う方法であって、
前記サービスサーバにて、必要なユーザ認証を終えていない前記クライアントからアクセスを受けた場合に、該クライアントに対して前記認証サーバにアクセスするよう要求するリダイレクト要求情報を送信し、
前記認証サーバにて、前記クライアントからアクセスがあった場合に該クライアントのユーザ認証を行い、前記ユーザ認証が成功した場合にユーザ認証が成功したことを表す情報を前記クライアントに送信する、
ことを特徴とするユーザ認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はユーザ認証機能付き通信システム及びユーザ認証方法に関し、特に、ネットワークに接続されたクライアント／サーバ間でのユーザ認証において認証サーバの汎用性を高める技術に関する。
【０００２】
【従来の技術】近年、ワールドワイドウェブ（WWW）を用いる通信環境が急速に普及しており、単なる学術レベルでの利用のみならず、オンラインショッピングや商用データベースサービス等、商業利用もまた急速に普及している。そして、このようにWWWを本格的に商業利用するには、Ｗｅｂサーバ側で信頼性の高いクライアントのユーザ認証を行う技術を確立することが必須であり、このため各種の技術が提案されている。
【０００３】図６は、WWWにおける従来一般的に考えられる認証サーバを持ったサービスサーバのクライアントの認証の仕組みを説明する図である。同図に示すように、WWWでは、Ｗｅｂブラウザを搭載したクライアント１００はインターネットにＵＲＬ（Uniform Resource Locater）を送出することにより、該ＵＲＬにより特定されるリソース（ハイパーテキスト）を取得し、ディスプレイ上に所望の画像表示を得ることができる。
【０００４】この際、クライアント１００がＵＲＬにより特定したリソースが、Ｗｅｂサービスサーバ１０２に格納されているものであり、ユーザ認証を必要とするサービスに関するものであれば、該Ｗｅｂサービスサーバ１０２はユーザＩＤやパスワード等の認証情報を求めるハイパーテキストをクライアント１００に送る。そして、これに応じてクライアント１００は所定の認証情報を該Ｗｅｂサービスサーバ１０２に送信する。
【０００５】こうして、クライアント１００から認証情報を受け取ったＷｅｂサービスサーバ１０２は、専用のアプリケーションインタフェース（ＡＰＩ）を用い、通常は同一ドメイン、すなわち同一ＬＡＮ環境に設置される認証サーバ１０４に対し、その受け取った認証情報を転送するとともに、ユーザ認証処理を依頼する。この依頼を受けた認証サーバ１０４は認証用データベース１０６に格納された各種認証情報を参照しつつユーザ認証を行う。そして、認証に成功して正規のユーザであると確認されれば、Ｗｅｂサービスサーバ１０２とクライアント１００とのその後の通信に供するよう、当該クライアント１００がユーザ認証済みであることを表すクッキー（Ｃｏｏｋｉｅ）を発行する。このクッキーは、Ｗｅｂサービスサーバ１０２からのハイパーテキストの返信に際して、そのヘッダ部分に含められる情報であり、以後、所定内容のクッキーを保持しているクライアント１００からのアクセスに対しては、Ｗｅｂサービスサーバ１０２は既にユーザ認証を終えているクライアント１００からのアクセスであると判断し、認証サーバ１０４でのユーザ認証を改めて行うことなく、ユーザ所望のハイパーテキストをクライアント１００に返信する。
【０００６】

【発明が解決しようとする課題】以上説明した従来一般のユーザ認証技術によれば、クライアント１００から送信された認証情報をもとにユーザ認証を行うことができ、WWWの商業利用に際して必要十分なセキュリティを確保することが可能となる。

【０００７】しかしながら、上記従来の技術によれば、認証サーバ１０４がＷｅｂサーバとして構築されたものではなく、フロントエンドとして用いられるＷｅｂサービスサーバ１０２とバックエンドとして用いられる認証サーバ１０４とが深い依存関係を必要とし、認証の依頼や結果通知のための専用のソフトウェアが両者にインストールされることが多い。このため、たとえ高機能な認証サーバ１０４を構築したとしても、これを他のＷｅｂサービスサーバ等で利用することは困難であり、認証サーバ１０４を複数のサービスで共通利用する効率的なシステムの構築が困難であった。

【０００８】本発明は上記課題に鑑みてなされたものであって、その目的は、サービスサーバと認証サーバとの独立性及び汎用性を高め、認証サーバを複数のサービスで共通利用することが容易な認証システムを提供することにある。

【０００９】

【課題を解決するための手段】（１）上記課題を解決するために、本発明は、ネットワーク上に相互に通信可能に接続されたサービスサーバ、認証サーバ、及びクライアントを含むシステムにおいて、前記サービスサーバは、必要なユーザ認証を終えていない前記クライアントからアクセスを受けた場合に、該クライアントに対して前記認証サーバにアクセスするよう要求するリダイレクト要求情報を送信する手段を含み、前記認証サーバは、前記クライアントからアクセスがあった場合に該クライアントのユーザ認証を行い、前記ユーザ認証が成功した場合にユーザ認証が成功したことを表す情報を前記クライアントに送信する手段を含む。

【００１０】（２）また、本発明の一態様では、前記認証サーバに含まれる前記手段は、ユーザ認証が成功したことを表す前記情報を前記クライアントに送信する際に、併せて前記サービスサーバにアクセスするよう要求するリダイレクト要求情報を送信する。

【００１１】（３）また、本発明のさらに他の態様では、前記クライアントは、前記サービスサーバ又は前記認証サーバからリダイレクト要求情報を受信した場合に前記認証サーバ又は前記サービスサーバにアクセスする手段を含む。

【００１２】（４）さらに、本発明の他の態様では、前記クライアントは、前記認証サーバから既に前記認証済み情報を受信している場合に、前記サービスサーバへのアクセスの際に前記認証済み情報を該サービスサーバに送信する手段をさらに含む。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態について図面に基づき詳細に説明する。

【００１４】図１は、本発明の実施の形態に係る認証システムの概略を説明する図である。同図において、Ｗｅｂシステムは、インターネット上に接続されたＷｅｂサービスサーバ１０及びクライアント１２と、同じくインターネットにファイアウォール１４を介して接続されたＷｅｂ認証サーバ１６と、を含んで構成されており、Ｗｅｂサービスサーバ１０とクライアント１２とＷｅｂ認証サーバ１６は相互に通信可能に接続されている。また、Ｗｅｂ認証サーバ１６は同一ＬＡＮ環境に設置された認証用データベース１８にアクセスすることができるようになっている。

【００１５】同図に示すＷｅｂシステムにおいて、Ｗｅｂブラウザを搭載したクライアント１２が未だ有効なユーザ認証を済ませていないＷｅｂサービスサーバ１０にアクセスした場合、該Ｗｅｂサービスサーバ１０はクライアント１２に対しリダイレクト要求を含むＷｅｂページを送信し、Ｗｅｂ認証サーバ１６に改めてアクセスするように要求する。クライアント１２ではこのリダイレクト要求を解釈し、図中矢印Ａに示すようにして、ユーザの干渉なしにＷｅｂ認証サーバ１６に自動的にアクセスする。

【００１６】多くのＷｅｂブラウザには、「リダイレクト要求」が含まれるハイパーテキストを受信した場合に、その要求を解釈して指定Ｗｅｂページを自動的にリロードすることができるようになっており、本認証システムではこの機能を積極活用することによって、Ｗｅｂサービスサーバ１０とＷｅｂ認証サーバ１６との直接的な通信を廃し、Ｗｅｂ認証サーバ１６の汎用性を高めることに成功している。

【００１７】その後、矢印Ａに示すようにして、クライアント１２がＷｅｂサービスサーバ１０の要求をリダイレクトしてＷｅｂ認証サーバ１６にアクセスすれば、Ｗｅｂ認証サーバ１６は認証用データベース１８に照らし合わせてユーザ認証を行う。

【００１８】ここでＷｅｂ認証サーバ１６にてユーザ認証に成功すれば、該Ｗｅｂ認証サーバ１６はクライアント１２に対してさらに別のリダイレクト要求を含むＷｅｂページを送信し、今度はＷｅｂサービスサーバ１０に改めてアクセスするように要求する。この際、このＷｅｂページにおいてはユーザ認証済みの旨を示す情報がクッキーに設定される。そして、このクッキーの内容を含んだＵＲＬをＷｅｂサービスサーバ１０が受け取ることにより、Ｗｅｂサービスサーバ１０はユーザが希望するＷｅｂページをクライアント１２に送信する。

【００１９】本認証システムにおいてはＷｅｂサービスサーバ１０からＷｅｂ認証サーバ１６へ直接のアクセスが発生しないため、それらＷｅｂサービスサーバ１０とＷｅｂ認証サーバ１６との間のインターフェースを非常

に簡潔なものとすることができる。これにより、サービスサーバと認証サーバとの独立性及び汎用性を高め、認証サーバを複数のサービスで容易に共通利用することができる。

【００２０】また、本認証システムでは、Ｗｅｂ認証サーバ１６及びＷｅｂサービスサーバ１０はいずれもインターネット上でＩＰアクセス可能なよう設置されていればよく、例えばＷｅｂ認証サーバ１６にはファイアウォール１４を介する以外に外部からアクセスできないようにしてもよい。さらに、Ｗｅｂ認証サーバ１６とＷｅｂサービスサーバ１０は従来技術のように必ずしも同一ＬＡＮ環境に設置する必要がない。このため、同じくインターネット上でＩＰアクセス可能なよう設置された他のＷｅｂサービスサーバ１０からもまた、同Ｗｅｂ認証サーバ１６に対して容易にユーザ認証を依頼することができる。

【００２１】以下、本認証システムの構成及び認証手順についてさらに詳細に説明する。

【００２２】図２は、Ｗｅｂサービスサーバ１０の構成を本通信システムの全体構成とともに示す図である。同図に示すように、Ｗｅｂサービスサーバ１０は、ｈｔｔｐｄ（Hyper Text Transfer Protocol Daemon）２０と、ファイル記憶部２２と、を有しており、ｈｔｔｐｄ２０には、データ受信部２４、データ解析部２６、データ処理部２８，３０、データ送信部３２、ｈｔｔｐｄ設定ファイル３４が設けられている。ここで、データ記憶部２４、データ解析部２６、データ処理部２８、データ送信部３２、ファイル受信部２２は従来一般のＷｅｂサーバに設けられているものと同様であり、データ処理部３０とｈｔｔｐｄ設定ファイル３４とが本実施の形態に係る認証システムを実現するために新たに追加された構成である。また、ファイル記憶部２２にはサービス内容たるＷｅｂページの他、ユーザ認証に失敗した旨を通知するための認証失敗ページに関するファイルが格納されている。また、データ処理部２８はｈｔｔｐｄ設定ファイル３４での設定により特に起動される実行モジュールであり、ｈｔｔｐヘッダの解析による従来一般のアクセス可否チェックを第１段階のセキュリティチェック機能として実現するとともに、第２段階のセキュリティチェック機能としてクライアント１２から受け取るクッキーの内容を基にしたアクセス可否チェックを行う。

【００２３】次に、図３はＷｅｂ認証サーバ１６の構成を示す図である。同図において、Ｗｅｂ認証サーバ１６の大部分の構成はＷｅｂサービスサーバ１０と同様であり、対応する構成には対応符号を付している。Ｗｅｂ認証サーバ１６には特に認証用データベース１８が接続されており、データ処理部３０ａは受信したＵＲＬが認証を要求するものである場合に該認証用データベース１８に問い合わせすることによりユーザ認証を行うことができるようになっている。

【００２４】本認証システムでは、まず、図２に示すＷｅｂサービスサーバ１０において、クライアントから送信されたＵＲＬがデータ受信部２４により受信され、Ｗｅｂサービスサーバ１０のデータ解析部２６は受信したＵＲＬから要求されているファイルの名称や各種変数等を取得する。その後、通常ならばデータ処理部２８によってサービス内容たる所定ファイルがファイル記憶部２２から読み出され、それが必要に応じて加工され、データ送信部３２によってインターネットに送出されるところ、本Ｗｅｂサービスサーバ１０では、ｈｔｔｐｄ設定ファイル３４によってデータ処理部３０が起動指定されており、該データ処理部３０によって２段階のアクセス可否チェックが施される。

【００２５】すなわち、データ処理部３０では、まず第１段階のアクセス可否チェックとしてｈｔｔｐヘッダの解析が行われ、ＵＲＬが一定範囲のＩＰアドレスから送信されたものであるのか、たとえばｊｐドメインを有するクライアントからの要求であるか等の事項がチェックされる。そして、ここでのチェックに適合しない場合には認証失敗の旨を表すＷｅｂページがクライアント１２に返信される。

【００２６】一方、このチェックに適合する場合、さらに第２段階のアクセス可否チェックが行われ、クライアント１２から受信するデータにクッキーが含まれているか、含まれているとして内容はどのようなものかが確認される。すなわち、本認証システムではＷｅｂ認証サーバ１６によって正常にユーザ認証が行われているクライアント１２に対してはユーザ認証済みの旨を表すクッキーが発行されるようになっており、ユーザ認証済みのクライアント１２からのアクセスに際してはそのクッキーがＷｅｂサービスサーバ１０に送信されるようになっている。

【００２７】そして、Ｗｅｂサービスサーバ１０ではクライアント１２からアクセスがあった場合に第２段階のアクセス可否チェックとしてそこから送信されてくるクッキーの内容を確認する。この確認によってユーザ認証済みの旨のクッキーを伴うアクセスであると判れば、クライアント１２に要求されたＷｅｂページを正常に返信する。一方、ユーザ認証済みの旨のクッキーを伴わないアクセスであると判れば、クライアント１２にＭＥＴＡタグ付きのＷｅｂページを送信するなどのリダイレクト要求を行う。このＭＥＴＡタグとはクライアント１２に対するリダイレクト要求情報のうちの１つであり、たとえば「<;META HTTP-EQUIV="Refresh" CONTENT="3; URL=Ｗｅｂ認証サーバ１６中の認証要求.html" >;」のような形式を有する。この例では、該要求がクライアント１２に到着してから３秒後にＷｅｂ認証サーバ１６に格納されている「認証要求.html」がアクセスされる。

【００２８】次に、図３に示すＷｅｂ認証サーバ１６においては、クライアント１２からリダイレクトして送信

されたＵＲＬがデータ受信部２４ａにより受け付けられ、データ解析部２６ａが受信したＵＲＬから要求されているファイルの名称や各種変数等を取得する。そして、クライアント１２からのアクセスが認証要求.htmlに対するものであれば、Ｗｅｂサービスサーバ１０と同様、データ処理部３０ａは、まず第１段階のアクセス可否チェックとしてｈｔｔｐヘッダの解析を行い、このチェックに適合しないアクセスに対しては、認証失敗の旨を表すＷｅｂページをＷｅｂサービスサーバ１０から取得するよう要求するＭＥＴＡタグを付したＷｅｂページをクライアント１２に送信する。このＭＥＴＡタグは、たとえば「<;META HTTP-EQUIV="Refresh" CONTENT="3; URL=Ｗｅｂサービスサーバ１０中の”認証失敗.html”>;」のような形式を有する。なお、この例では、該要求がクライアント１２に到着してから３秒後にＷｅｂサービスサーバ１０に格納されている「認証失敗.html」がアクセスされる。

【００２９】一方、第１段階のアクセス可否チェックをクリアした場合には、さらにデータ処理部３０ａはクライアント１２のユーザ認証を行う。ユーザ認証の方法はたとえばＷｅｂ認証サーバ１６がクライアント１２からユーザＩＤやパスワード等の認証情報を送信するよう要求してもよいし、また、Ｗｅｂサービスサーバ１０側で予めクライアント１２から所定の認証情報を受信しておき、それをクッキーヘッダに設定するなどの方法によりＷｅｂサービスサーバ１０からＷｅｂ認証サーバ１６へのリダイレクト要求によってクライアント１２を介してＷｅｂ認証サーバ１６に転送するようにしてもよい。Ｗｅｂ認証サーバ１６のデータ処理部３０ではこうして得られる認証情報を基に適宜認証用データベース１８に問い合わせすることにより、ユーザ認証を行う。

【００３０】そして、ユーザ認証に失敗すれば、データ処理部３０ａは、Ｗｅｂサービスサーバ１０に格納されている認証失敗の旨を表すＷｅｂページにアクセスするよう、所定のＵＲＬをファイル格納部から読み出し、クライアント１２にそのＵＲＬへのリダイレクト要求を行うＷｅｂページを送信する。一方、ユーザ認証に成功すれば、データ処理部３０は、Ｗｅｂサービスサーバ１０に格納されている所定Ｗｅｂページにアクセスするよう、所定のＵＲＬをファイル格納部から読み出し、クライアント１２にそのＵＲＬへのリダイレクト要求を行うＷｅｂページを送信する。この際、この送信するＷｅｂページのヘッダにおいてはユーザ認証済みの旨を表すクッキーが設定される。

【００３１】こうすれば、この後クライアント１２がＷｅｂサービスサーバ１０にアクセスする場合には、ユーザ認証済みの旨を表すクッキーが併せて送信されることになり、改めてユーザ認証を行うことなく、クライアント１２のユーザは所望のＷｅｂページを正常にＷｅｂサービスサーバ１０から受け取ることができる。

【００３２】ここで、Ｗｅｂサービスサーバ１０からＷｅｂ認証サーバ１６への問い合わせが発生するケースについて、図４に示す通信シーケンス図に基づいて認証手順を説明する。

【００３３】まず、クライアント１２のユーザがＷｅｂサービスサーバ１０に対するサービスを要求するＵＲＬを入力すれば（Ｓ１０１）、クライアント１２にてそのＵＲＬをインターネットに送出する（Ｓ１０２）。その後、Ｗｅｂサービスサーバ１０にてアクセス可否の確認が行われる（Ｓ１０３）。そして、上述した第２段階でのアクセス可否チェックにおいて、クライアント１０からのアクセス要求が必要なクッキーを備えないものであると判断された場合は特に、Ｗｅｂサービスサーバ１０からクライアント１２にリダイレクト要求を含むＷｅｂページが送信される（Ｓ１０４）。

【００３４】これを受けてクライアント１２は、そのリダイレクト要求に従ってＵＲＬをインターネットに送出し、Ｗｅｂ認証サーバ１６にアクセスする（Ｓ１０５）。Ｗｅｂ認証サーバ１６では、上述した第１段階のアクセス可否チェックを行うとともに、ユーザ認証を行う（Ｓ１０６）。

【００３５】そして、ユーザ認証に成功すれば、認証済みの旨の情報をクッキーに設定し、再びＷｅｂサービスサーバ１０にアクセスするようリダイレクト要求を含むＷｅｂページをクライアント１２に送信する（Ｓ１０７）。この際、ユーザ認証に失敗した場合は、ユーザ認証に失敗した旨を表す情報をクッキーに設定して所定のＷｅｂページをクライアント１２に返信するようにしてもよい。こうすれば、たとえばＷｅｂサービスサーバ１０にてユーザ認証に失敗したクライアント１２からのアクセスを速やかに判別することができる。

【００３６】その後、クライアント１２ではＷｅｂ認証サーバ１６から受信したＷｅｂページに含まれているリダイレクト要求に従い、再びＷｅｂサービスサーバ１０にアクセスする（Ｓ１０８）。このアクセスではクライアントから送信されるＵＲＬに認証済みの旨のクッキーが含まれており、Ｗｅｂサービスサーバ１０はユーザ認証を正規に終えたクライアントからのアクセスであると判断し（Ｓ１０９）、ユーザ所望のＷｅｂページをクライアント１２に返信する（Ｓ１１０）。そして、クライアント１２では受信したＷｅｂページを解釈してディスプレイ表示を行う。

【００３７】なお、上述のように、ユーザ認証に失敗した旨のクッキーをＷｅｂ認証サーバ１６で設定するようにした場合には、Ｗｅｂサービスサーバ１０は、Ｓ１１０において、かかるクッキーを伴うアクセスに対しアクセス拒否の旨のＷｅｂページ等を返信するようにしてもよい。

【００３８】また、以上のようにして正規の認証済み情報がクッキーとして記録されているクライアント１２か

ら、その後Ｗｅｂサービスサーバ１０にアクセスがあった場合には、Ｗｅｂサービスサーバ１０はＷｅｂ認証サーバ１６への問い合わせを行わない。図５は、かかるケースでのクライアント１２とＷｅｂサービスサーバ１０との間の通信を説明する通信シーケンス図である。

【００３９】同図に示すように、クライアント１２のユーザがＷｅｂサービスサーバ１０に対するサービスを要求するＵＲＬを入力すれば（Ｓ２０１）、クライアント１２にてそのＵＲＬをインターネットに送出する（Ｓ２０２）。この際、クライアント１２には既にユーザ認証済みの旨のクッキーが記録されており、Ｗｅｂサービスサーバ１０に送信されるＵＲＬにはその記録されたクッキーの内容が含められる。その後、Ｗｅｂサービスサーバ１０にてアクセス可否の確認が行われる（Ｓ２０３）。

【００４０】そして、このケースのアクセスでは、上述した第２段階でのアクセス可否チェックにおいて必要なクッキーを備えているアクセスであると判断されるため、ユーザ所望のＷｅｂページに関するデータが正常にクライアント１２に送信される（Ｓ２０４）。そして、クライアント１２では受信したＷｅｂページを解釈してディスプレイ表示を行う。

【００４１】なお、以上説明した認証システムは種々の変形実施が可能である。

【００４２】たとえば、ユーザ認証済みの旨を表すクッキーにはそのユーザ認証の有効期限を表す情報を設定するようにしてもよい。こうすれば、Ｗｅｂサービスサーバ１０はクライアント１２からユーザ認証済みの旨を表すクッキーを受け取ったとしても、それが有効期限を過ぎたものであれば、必要に応じて、再びＷｅｂ認証サーバ１６にアクセスしてユーザ認証を行うようクライアント１２に要求することができる。

【００４３】また、上記説明では、クライアント１２、サービスサーバ、認証サーバがインターネットにされたものであり、それらがＨＴＴＰプロトコルに従うものであることを前提にしたが、本発明はプロトコルやネットワークの形態によらず、必要な構成を備えるすべてのネットワーク形態に適用可能なものである。

【００４４】

【発明の効果】以上説明したように、本発明によればサービスサーバと認証サーバとの間での直接アクセスを廃し、ユーザ認証をクライアントと認証サーバとの間で直接に行わせるようにしたので、サービスサーバと認証サーバとの相互依存関係を少なくすることができる。このため、認証サーバの汎用性を高めて複数のサービスサーバで該認証サーバを共用することが可能となる。

【００４５】また、本発明によれば、認証サーバが認証済み情報をクライアントに送信する際にリダイレクト要求情報を併せてクライアントに送信するようにしたので、クライアントからサービスサーバへ再度アクセスする際のタイミングを認証サーバから提供することができる。この結果、たとえばクライアント１２はこのリダイレクト要求情報の受信をトリガとして再びサービスサーバへアクセスすることが可能となる。

【００４６】また、本発明によれば、クライアントがサービスサーバからリダイレクト要求情報を受信した場合にクライアントが自動的に認証サーバにアクセスするようにしたので、クライアントのユーザが特段の操作をすることなくユーザ認証を進めることができる。

【００４７】また、本発明によれば、クライアントが認証サーバからリダイレクト要求情報を受信した場合にクライアントが自動的にサービスサーバにアクセスするようにしたので、ユーザ認証を無事に終えたクライアントのユーザが特段の操作をすることなく再びサービスサーバにアクセスすることができる。

【００４８】また、本発明によれば、クライアントが既に認証済み情報を受け取っている場合、サービスサーバへのアクセスの際にその認証済み情報を該サービスサーバに送信するようにしたので、サービスサーバ側でそのクライアントがユーザ認証に成功したものであることを知ることができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態に係る通信システムの全体構成を示す図である。

【図２】　本発明の実施の形態に係るＷｅｂサービスサーバを通信システムの全体構成とともに示す図である。

【図３】　本発明の実施の形態に係るＷｅｂ認証サーバの構成を示す図である。

【図４】　Ｗｅｂサービスサーバからｗｅｂ認証サーバへの問い合わせの様子を説明する通信シーケンス図である。

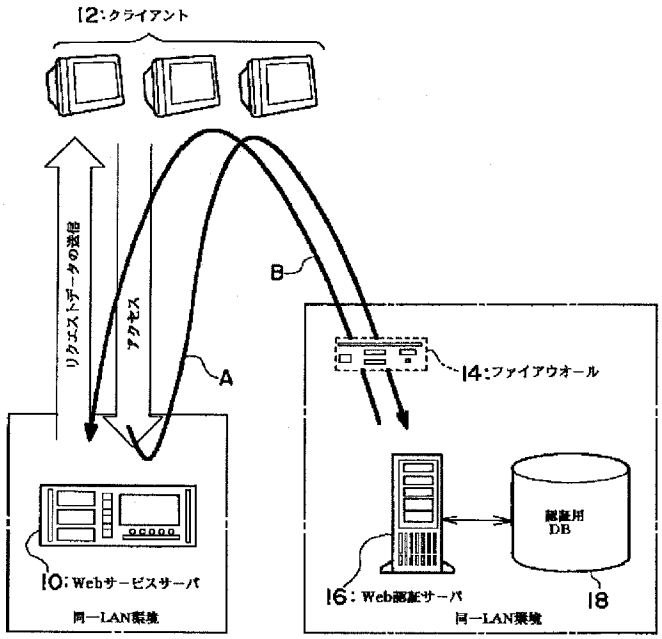
【図５】　ユーザ認証を正常に終えたクライアントとＷｅｂサービスサーバとの通信を説明する通信シーケンス図である。

【図６】　従来技術に係るユーザ認証の仕組みを説明する図である。

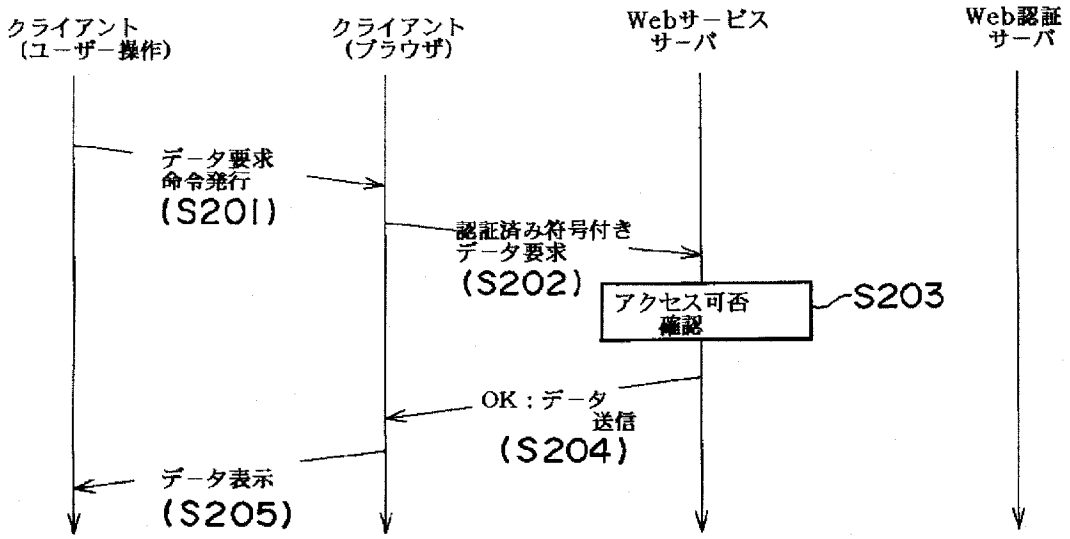
【符号の説明】

１０　Ｗｅｂサービスサーバ、１２　クライアント、１６　Ｗｅｂ認証サーバ、１８　認証用データベース。

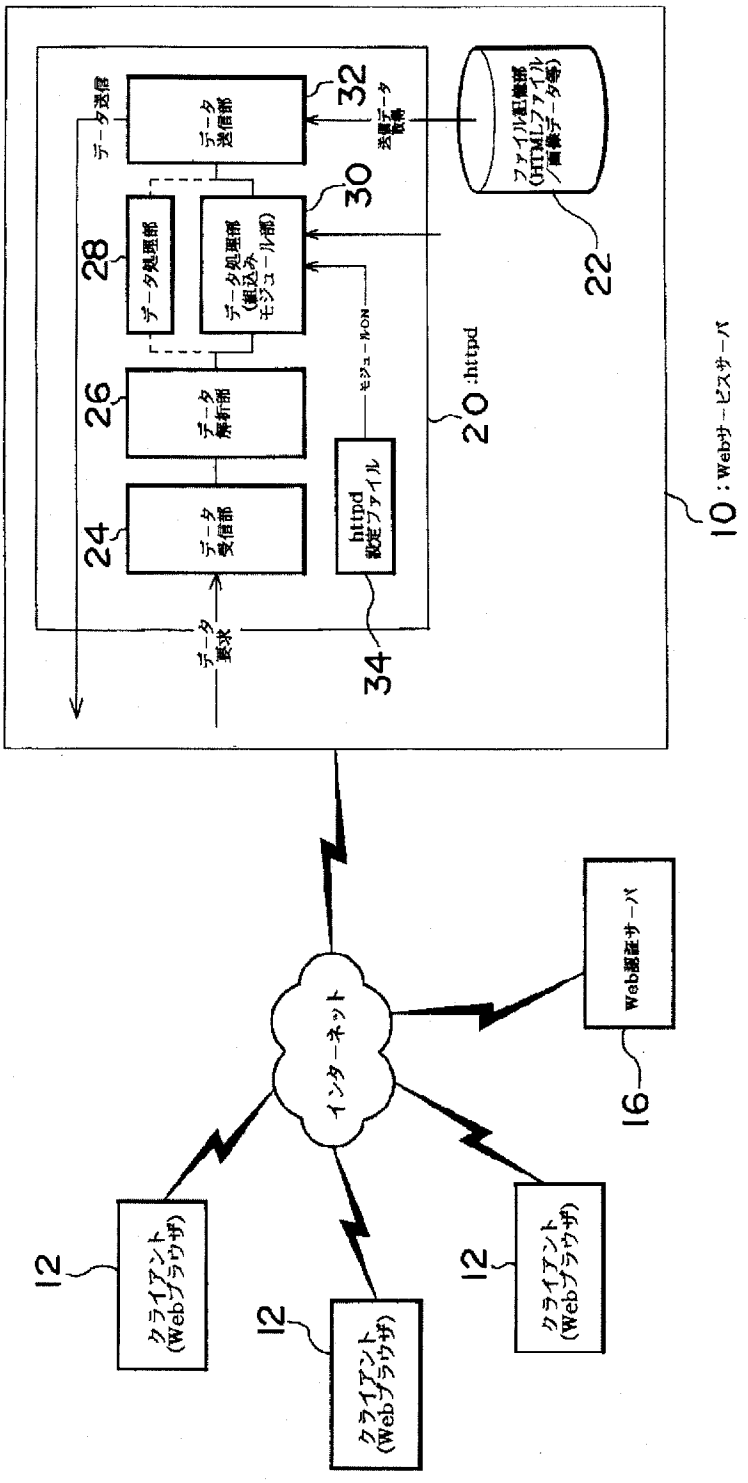
【図１】


12:クライアント
リクエストデータの送信
アクセス
A
B
14:ファイアウオール
認証用
DB
10:Webサービスサーバ
同一LAN環境
16:Web認証サーバ
18
同一LAN環境

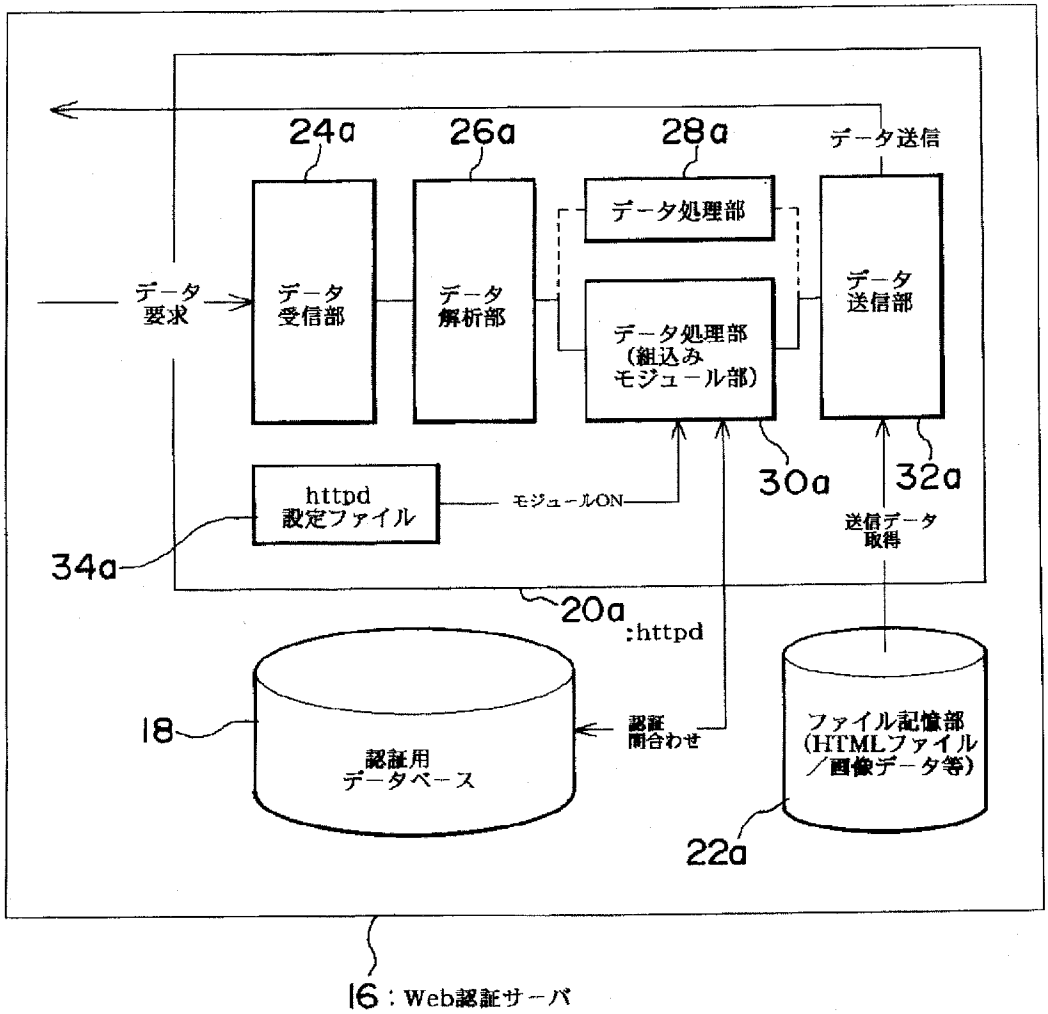
【図５】


クライアント
(ユーザー操作)
クライアント
(ブラウザ)
Webサービス
サーバ
Web認証
サーバ
データ要求
命令発行
(S201)
認証済み符号付き
データ要求
(S202)
アクセス可否
確認
S203
OK：データ
送信
(S204)
データ表示
(S205)

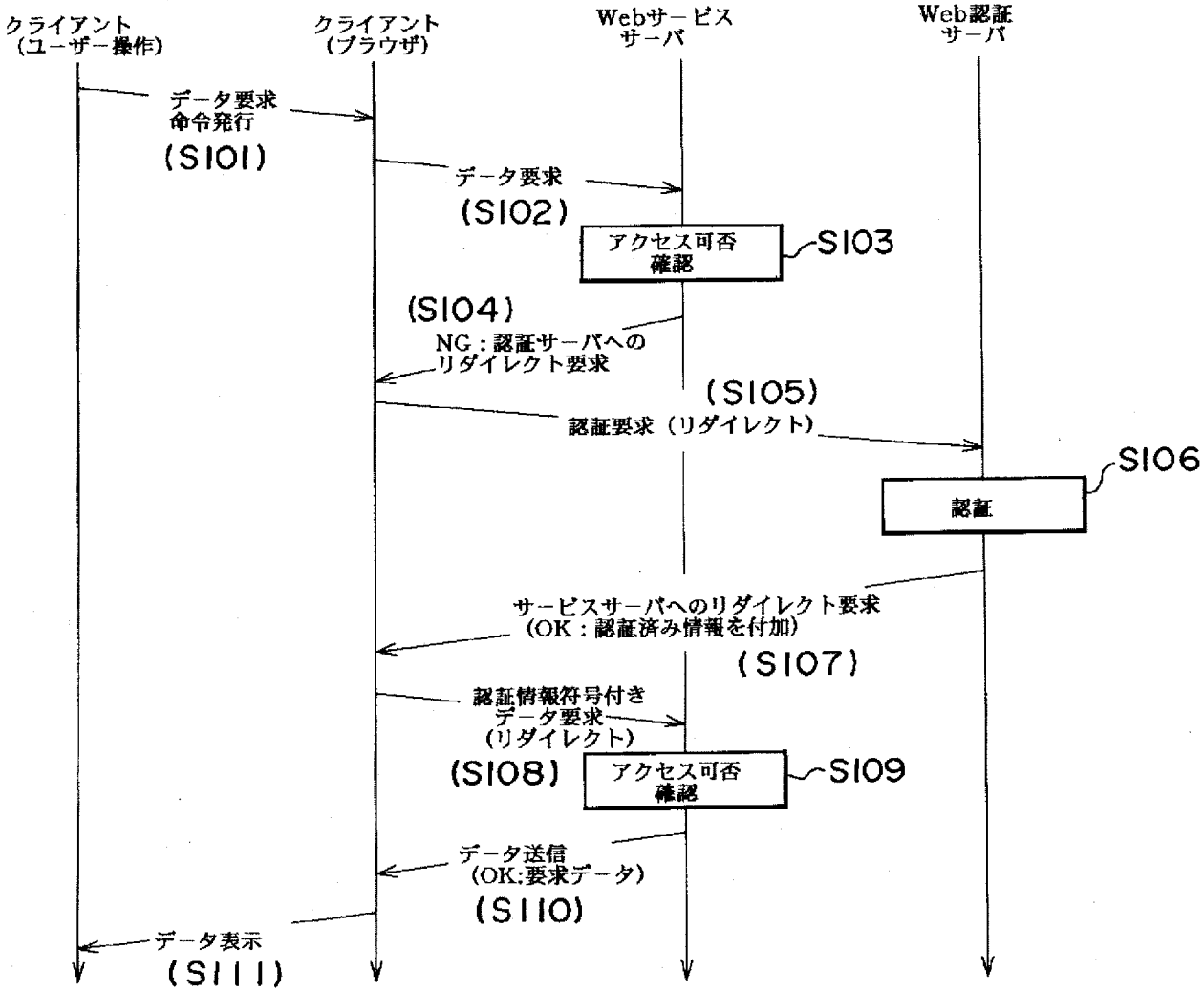
【図２】


10：Webサーバシステム
20：httpd
22
24
26
28
30
32
34
データ送信部
データ処理部
データ処理部（組込み型モジュール部）
データ解析部
データ受信部
httpd設定ファイル
ファイル記憶部（HTMLファイル／画像データ等）
データ送信
送信データ取得
データ要求
モジュールON
インターネット
Web認証サーバ
16
クライアント（Webブラウザ）
12
12
12

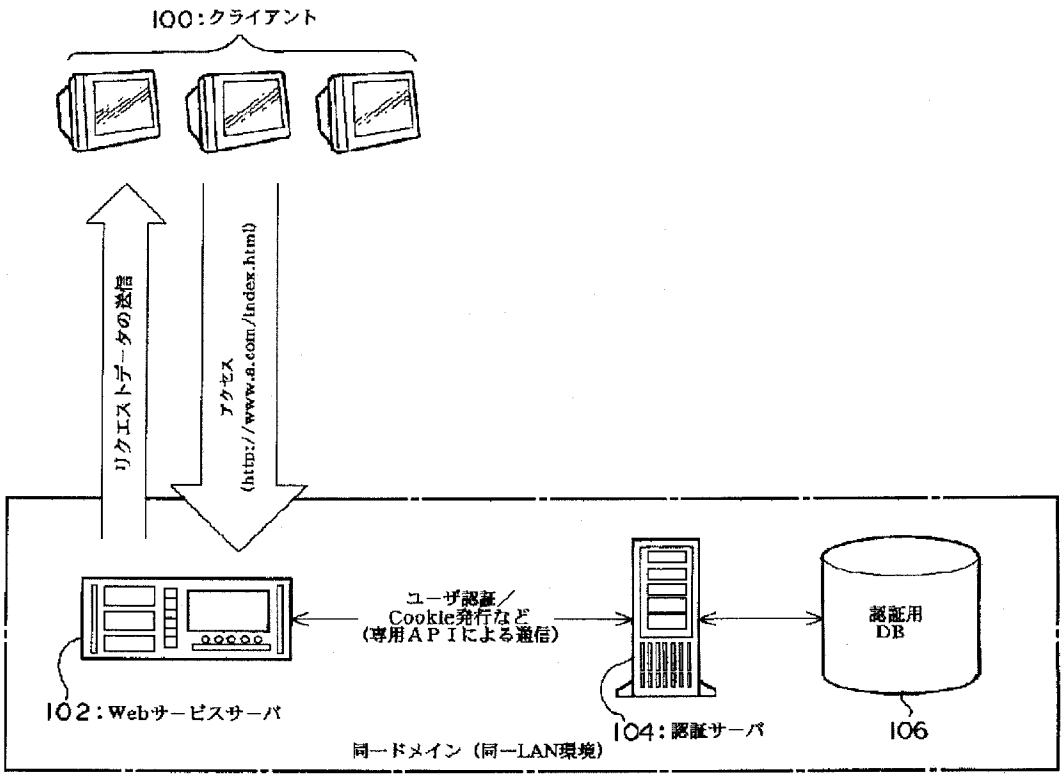
【図３】


24a
26a
28a
データ送信
データ処理部
データ
要求
データ
受信部
データ
解析部
データ処理部
（組込み
モジュール部）
データ
送信部
httpd
設定ファイル
モジュールON
30a
32a
送信データ
取得
34a
20a
:httpd
18
認証用
データベース
認証
問合わせ
ファイル記憶部
（HTMLファイル
／画像データ等）
22a
16：Web認証サーバ

【図４】


クライアント
(ユーザー操作)
クライアント
(ブラウザ)
Webサービス
サーバ
Web認証
サーバ
データ要求
命令発行
(S101)
データ要求
(S102)
アクセス可否
確認
S103
(S104)
NG：認証サーバへの
リダイレクト要求
(S105)
認証要求（リダイレクト）
S106
認証
サービスサーバへのリダイレクト要求
(OK：認証済み情報を付加)
(S107)
認証情報符号付き
データ要求
(リダイレクト)
(S108)
アクセス可否
確認
S109
データ送信
(OK:要求データ)
(S110)
データ表示
(S111)

【図６】


100：クライアント
リクエストデータの送信
アクセス
(http://www.a.com/index.html)
ユーザ認証／
Cookie発行など
（専用ＡＰＩによる通信）
認証用
DB
102：Webサービスサーバ
104：認証サーバ
106
同一ドメイン（同一LAN環境）